REMARKS

This application has been carefully reviewed in view of the above-referenced Office Action in which new grounds for rejection have been presented. Reconsideration is requested in view of the following remarks.

REQUEST FOR INTERVIEW

The undersigned again respectfully requests the courtesy of an interview.

Response to section 3 of the Office Action

The Office asserts that there are multiple failures in disclosure in the specification. In particular, at the top of page 3, the Office asks "why are the already transferred keys lost?". The nature of the question itself suggests that there is not a full understanding of the process and the undersigned respectfully submits that the Examiner's time would be well spent studying the specification and related documents in detail. Applicant has explained the problems that are being addressed in great detail in the background coupled with the first several pages of the detailed description. For example, one answer to the Office's question can be found in the paragraphs from line 12 of page 12 through line 3 of page 14. Namely (to briefly summarize), in one example, if the encryption system resets or loses communication with the CA management system, it has no idea what to encrypt or what keys to use. In real world systems, this results in transmission of content without it being encrypted. Known real world encryption systems by default have no encryption enabled. They must be configured to provide encryption to specified content, hence, without such configuration the content is transmitted by default in the clear. Although keys are not lost at the receiving end, they may be stale due to the rapidity with which certain keys are changed. It takes a period of time for the CA management system to initialize the encryption process (sometimes even to learn that there has been a failure resulting in lack of encryption) and during this time, content is transmitted without encryption. At a receiving device, if the device receives unencrypted content, it treats it as unencrypted. Hence, content such as adult material or pay-per-view content may be sent and received without benefit of encryption.

The Office asserts that there is not a claim limitation to "always assure" encryption of content. The claims have been amended to address this more clearly.

Regarding the rejections under 35 U.S.C. §112

The Office rejects claims 1, 9, 16, 23, 29, 35, 41, 47 and 52 as failing to comply with the written description requirement. Applicant strenuously traverses this rejection, but has made amendments in an earnest attempt to reach common ground with the Examiner.

The Office submits that in claims 1, 9, 16, 23, 29, 35, 41, 47 and 52 the language about the default encryption key being distinct from keys supplied by the conditional access management system is not reasonably conveyed in the description. Applicant respectfully but strenuously disagrees. The specification clearly discloses in multiple places that the default key is a "fixed key" (e.g., page 17, starting at line 11) as opposed to a live key or active key as well as providing additional distinctions. Those familiar with CA systems recognize that live keys or active keys (or code words) are conventionally generated on a periodic basis and updated to thwart hackers. Some level of detailed explanation of this process is provided at about page 3 of the specification. This is clearly the "normal" mode of operation of a CA system. Those skilled in the art will have no difficulty in understanding the claim language as submitted.

Additionally, it is noted that although the terms used in the claims may not be supported verbatim, there is no requirement that they be supported in this manner so long as the equivalent meaning is conveyed in the specification. (See MPEP 2163 - *Martin v. Johnson*, 454 F.2d 746, 751, 172 USPQ 391, 395 (CCPA 1972) (stating "the description need not be in *ipsis verbis* [i.e., "in the same words"] to be sufficient")

This notwithstanding, the claims have been amended to describe the "normal" keys as "live" keys that are periodically changed and that the default keys are "fixed" keys (see spec. at about page 17, line 17). The claims have also been clarified to specify that the memory stores "fixed default encryption information for use by the conditional access encryption system to encrypt certain categories of audio/video content that are always to be encrypted". Page 14, first full paragraph delineates examples of such categories of A/V content (e.g., Pay-per-view, subscription, VOD, Adult or otherwise objectionable content). The original claim language

encompassed this concept by use of the term "certain audio/video content", however, it is believed that this clarification will assist the examiner in understanding the intended meaning. The nature of the memory as being non-volatile (page 14, line 5) is also incorporated and the dependent claims that formerly introduced that feature have been cancelled.

With these explanations and amendments, the claims are submitted to more than fully comply with 35 U.S.C. §112, and the Office's response to Applicants Arguments are believed fully addressed. Reconsideration and allowance are respectfully requested.

Regarding the Rejections under 35 U.S.C. §103

Claims 1-57 are rejected as being unpatentable over Maillard in view of Bestler and Yonge, all of record.

In order to establish *prima facie* obviousness, the Office Action must establish the presence of each claim feature of in the cited art and provide articulated reasoning with rational underpinning for the obviousness of the combination of claim features and their interrelationship. The Office Action admits that Maillard does not specifically disclose the encryption of certain content upon a communication failure between the conditional access (CA) management system and the conditional access encryption system and looks to Bestler to remedy this lack. The Office Action seems to assert that these claim features are met by Bestler at col. 3, lines 1-6, col 5, lines 19-22, col. 5, lines 37-39 and col. 5, lines 60-63, however, they are not. The Office asserts that Yonge discloses default decryption, but also fails to address any condition of the communication between the CA management system and the CA encryption system. This claim feature is totally unaddressed in the known prior art.

The Maillard reference of record describes a conditional access system that uses smart cards at the receiver for decryption functions. As is apparently acknowledged by the Examiner, Maillard does not disclose encrypting certain content using a default key in the event of a communication failure (see paragraph spanning pages 3 and 4), and in particular fails to disclose, teach or suggest any action that should occur in the event of a "communication failure between the conditional access encryption system and the conditional access management system in which said communication failure results in an inability for the conditional access management

system to provide the live encryption keys to the conditional access encryption system which would otherwise result in the audio/video content being distributed unencrypted" (emphasis added) as claimed for example in claim 1. The Office seems to assert that Maillard discloses a default encryption mechanism, but the undersigned is unable to find any such disclosure.

The Bestler reference of record, as understood, describes use of session data packets that are alternately encrypted/decrypted with two different session keys (col.3, lines 1-6). When a new key (a third key) is provided by the headend, one of the old keys continues to work for a time, while the other is rendered obsolete. New keys can thereby be introduced periodically as desired to enhance the system's security (col. 5, lines 19-22). But still, there is no disclosure, teaching or suggestion of a in the event of a "communication failure between the conditional access encryption system and the conditional access management system in which said communication failure results in an inability for the conditional access management system to provide the live encryption keys to the conditional access encryption system which would otherwise result in the audio/video content being distributed unencrypted" as claimed for example in claim 1. The only discussion of a communication failure relates to an inability to poll all subscribers in an IPPV environment. This has nothing to do with a communication failure between a CA management system and a CA encrypter.

The Yonge reference discloses a default key, as noted at col 33, lines 7-17 the key is used to secure communication between multiple stations in a CSMA network (abstract). However, as with the remainder of the references, Yonge fails to disclose, teach or suggest any action that should take place in the event of a failure in communication between a CA management system and a CA encryption system as claimed. Hence, none of the cited references alone or in combination discloses, teaches or suggests any action that should take place in the event of a communication failure between the CA management system and the CA encryption system. Absent a teaching relating to such communication failure, there can be no finding of obviousness. Each and every claim presented for examination calls for an action responsive to such a specific failure. The Office has not found any art that singly or collectively addresses this conditional action and hence all claims are submitted to be allowable. Reconsideration and allowance are respectfully requested.

Additionally, in order to properly combine references to establish *prima facie* obviousness, it is the burden of the Office to identify each element of the claims in the prior art and further, to provide an explicit analysis as to the reasoning to support a conclusion of obviousness. (See *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006) - "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

The Office argues in certain instances that the combination proposed would be obvious because one would have been motivated to employ the teachings of the cited references in order to ensure efficient station-to-station dialog or QOS. However, the Office provides no explanation as to how the proposed combination would accomplish efficient station-to-station dialog or QOS. There is no indication that the communication method which Applicants have modified fail to provide efficient station-to-station dialog (in fact, no such dialog at all is provided in encrypted cable television systems) and no nexus has been made to any improvement in QOS provided by the combination (note that QOS generally refers to the quality of data transmission – one could argue that imposing encryption actually inhibits QOS in that it inhibits reception by certain stations). Moreover, in the case of digital TV CA encryption there is no station to station communication – all communication is between a station and the headend.

In other instances, the Office argues that the combination would permit a subscriber to self-authorize pay TV, but again the undersigned finds no nexus between the proposed motivation and the actual claimed combination. Applicants do not understand how the claims enable self authorization.

In order to establish *prima facie* obviousness, the Office is obligated to provide an articulated reasoning for making the proposed combination. The Office cannot simply find a collection of similar elements and assert the proposed combination to be obvious in the absence of such an articulated reasoning based upon evidence. The reasoning supplied is clearly inadequate since nothing addresses how one assures that there is always encryption on certain content, and there is no explanation as to how the proposed combination would even accomplish that which is asserted to be motivated.

Maillard does not disclose encryption methods responsive to a communication failure, Bestler provides for certain communication failures, but not the communication failure addressed and specifically claimed, and Yonge only provides for a default encryption key used in inter-station communication. No viable articulated reasoning is provided that would put these pieces together in a manner that always assures some degree of protection by encryption. Hence *prima facie* obviousness has not been established.

The Office is further obligated to find all claim features arranged as claimed in order to establish *prima facie* obviousness. In view of the present amendments and arguments, it is submitted that the proposed rejections are inadequate. Reconsideration and allowance are respectfully requested.

In view of these amendments, all claims are submitted to be allowable for at least the reasons discussed above. Accordingly, reconsideration and allowance are respectfully requested.

Concluding Remarks

The undersigned additionally notes that many other distinctions exist between the cited art and the claims. However, in view of the clear distinctions pointed out above, it is submitted that further discussion is unnecessary. Applicant reserves the right to present further arguments at a later date for any of the rejected claims, but feels that the present arguments adequately address the rejections at hand.

Respectfully submitted,

/Jerry A. Miller 30779/

Jerry A. Miller
Registration No. 30,779

Dated: 7/1/2009

Please Send Correspondence to:
Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606
Phone: (919) 816-9981
Fax: (919) 816-9982
Customer Number 24337